Оперативная сводка

Оперативник «Призрак» прибывает в линейный город М. В городе М. орудуют две преступные группировки:

Уситора

Cipher-text

Призрак

Сэйбэя

«Призрак» намерен прекратить преступную деятельность на территории города, но ему необходимо узнать, где будет происходить очередная встреча представителей группировок.

Что на данный момент известно оперативнику:

- Любой обмен сообщениями между группировками происходит по защищённому каналу, то есть все сообщения шифруются:
- Все сообщения - это документы формата .docx которые максимально просты в оформлении, то есть не содержат стилей, тем;
- Алгоритм шифрования данных.

Алгоритм шифрования

Пусть M - файл который необходимо зашифровать. Далее каждый файл будем рассматривать в виде битовой строки (в бинаром виде) $M = m_0, m_1, \ldots, m_t$, где $t \in \mathbb{N}, m_i \in \overline{0,1}, i \in \overline{0,t}$. У группировок Уситора и Сэйбэя есть общий ключ шифрования $K \in V_{64}$ - битовая строка длины 64.

Тезисно

Шифрование файла M осуществляется следующим образом: к каждому биту полученного текста прибавляется по модулю 2 бит гаммы (т.е. к каждому биту с помощью операции XOR прибавляется бит который вырабатывает шифратор). Файл $M = m_0, m_1, \ldots, m_t$, в зашифрованном виде это битовая строка (файл в бинарном представлении):

$$m_0 \oplus \gamma_0, m_1 \oplus \gamma_1, \ldots, m_t \oplus \gamma_t,$$

где $t \in \mathbb{N}, m_i \in \overline{0,1}, i \in \overline{0,t}$.

Подробно

Рассмотрим линейную реккуренную последовательность (ЛРП) с характерестическим многочленом $h(x) = x^{64} \oplus x^{63} \oplus x^{12} \oplus 1$ начальное заполнение которой является ключом K. Обозначим начальное заполнение ЛРП как

$$(u_{63}, u_{62}, \dots u_0), u_j \in \{0,1\}, j = \overline{0,63},$$

а значение ЛРП на i-ом шаге как

$$(u_{63+i}, u_{62+i}, \dots u_i), u_{j+i} \in \{0,1\}, j = \overline{0,63},$$

при этом если состояние на i-ом шаге ЛРП следующее

$$(u_{63+i}, u_{62+i}, \dots u_i), u_{j+i} \in \{0,1\}, j = \overline{0,63},$$

то на $i + 1$ шаге оно будет таким:

$$(u_{62+i}, u_{61+i}, \dots u_{i+1}, u_i, r), \text{ где } r = u_{63+i} \oplus u_{12+i} \oplus u_i.$$

Преобразование выглядит как сдвиг, но один из символов равен сумме некоторых остальных. Знак гаммы на i-ом шаге вычисляется следующим образом:

$$\gamma_i = f((u_{63+i}, u_{62+i}, \dots u_i)), \text{ где}$$

$$f(x_{63}, x_{62}, \dots, x_0) = x_{63} \oplus x_{61} \oplus x_{59} \oplus x_{12} \oplus x_2 \oplus x_0 \oplus x_3 \cdot x_4,$$

то есть знак гаммы это значение нелинейной булевой функции от текущего входа ЛРП.

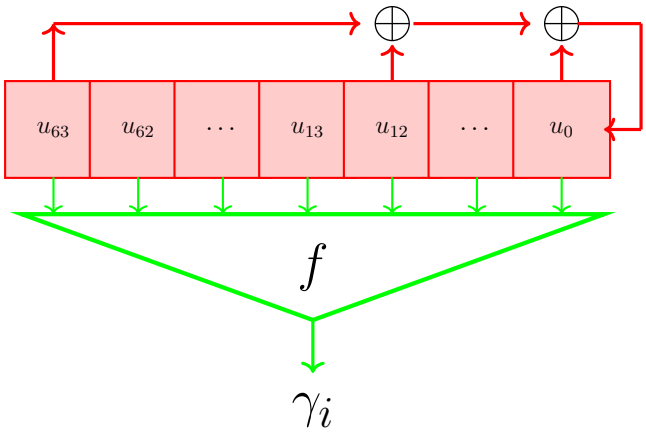

Рис. 1: Алгоритм шифрования схематично


Инстинкты и слабости как раз и отличают нас от мерзких машин.